REMARKS

Claims 1-51 are pending in the present application. In the above amendments, claims 1, 3, 11, 14, 16, 19, 22, 26, 50, and 51 have been amended to clarify the claimed subject matter. No new claims have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 112

The Office Action rejected claims 10 and 15 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement as there is no mention in the specification of preventing retransmission of the second private key. Applicant respectfully disagrees. Paragraph [0035] of the published application states "[t]he second private key is output (230) *once* at the request of the owner of user device 110. *Thereafter, user device 110 does not respond to such requests.*" In other words, as the second private key is only output once and the user device does not respond to additional requests for the second private key, *retransmission of the second private key is prevented.* Consequently, this rejection is moot.

The Office Action rejected claim 7 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Office action alleges that it is not possible for the second public and private keys to be created independently from the first public and private keys and that the second private key is associated with the first private key. Specifically, the Office Action states that it "is not possible for the two to be independent when earlier they are defined as being associated." Applicant respectfully disagrees with this analysis. Claim 7 indicates that the second public and private keys are *created independently* from the first public and private keys and not that the second public and private keys are independent of the first public and private keys. It is possible for two elements to be created separately but yet still be associated. In this case, the second public and private keys were not *created with the first public and private keys but were* created separately, i.e. created independently. Consequently, the first and second public and private keys can be created independently but yet still associated with each other. As a result, this rejection is moot.

Claim Rejections – 35 USC § 101

The Office Action rejected claims 14-21 and 40-42 under 35 U.S.C. §101 because the invention is alleged to be directed to non-statutory subject matter since the specification defines the means to include software only [0064] . Applicant respectfully disagrees. Paragraph [0064] of the published application includes that "embodiments may be implemented by hardware, software, firmware, middleware, microcode or any combination thereof." The hardware may include, for example, a processor, a storage medium, a transmitter, and/or a receiver which are illustrated in Figure 1 of the present application. The "means for .." limitations in these claims may be implemented by, for example, a processor performing the claimed functions. Consequently, these claims are directed to statutory subject matter.

Claim Rejections – 35 USC § 103

The Office Action rejected independent claims 1, 11, 14, 19, 22, 26, 50 and 51 under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 6,959,393 to Robert L. Hollis et al. (hereinafter "Hollis") in view of U.S. Patent Publication No. 2002/0152380 to Gregory O'Shea et al (hereinafter "O'Shea"). Claims 2-6, 8-10 and 23-25 are rejected under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 6,959,393 (hereinafter "Hollis") in view of Bruce Schneier's Applied Cryptography (hereinafter "Schneier"). Claims 29, 30, 33, 34, 36, 37, 40, 41, 43, 44, 47 and 48 are rejected under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 7,162,037 to Joerg Schwenk (hereinafter "Schwenk") in view of Bruce Schneier's Applied Cryptography (hereinafter "Schneier"). Claims 31, 32, 35, 38, 39, 42, 45, 46 and 49 are rejected under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 7,162,037 to Joerg Schwenk (hereinafter "Schwenk") in view of O'Shea and further in view of U.S. Patent No. 6, 263,437 Hanquing Liao et al (hereinafter "Liao"). Theses rejections are respectfully traversed in its entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. In re Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (a) determining the scope and content of the prior art; (b) ascertaining the differences between the claimed invention and the prior art; (c) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (d) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966).

Applicants respectfully submit that the present claims are not obvious in view of the cited references under a *Graham* analysis. More specifically, one of ordinary skill in the art would not arrive at Applicant's claimed invention in view of the differences between the cited reference and the presented claims.

By way of illustration, but not limiting the scope of the claims, Applicants disclose a system and method for *authentication* of subscriber user devices (e.g., mobile phones) with a network verifier. Each mobile user device generates its own first public-private key pair (and a backup or second public-private key pair) and *wirelessly distributes* the public key to the verifier for future *authentication* of the mobile user device. A *plurality of shares* of the second private key are wirelessly transmitted to *a plurality of different entities once* such that the second private key can be *re-created by the mobile user device to replace use of the first private key* and *disable the first private key when the second private key is re-created.*

Claims 1, 11, 14, 19, 22, 26, 50 and 51

As to independent claims 1, 11, 14, 19, 22, 26, 50 and 51, Office Action cites Hollis as teaching the claimed invention except for "creating the keys at a mobile device, wirelessly transmitting the keys, and then authenticating at the mobile device."

To clarify the focus of the present claims 1, 14, 22, 26, and 50 have been amended to more clearly recite various features.

Differences Between Prior Art and Claims: Claimed Elements are Not Taught by the Prior Art

Applicant submits that neither Hollis nor O'Shea teach the claimed limitations (1) a mobile user device is authenticated by a network verifier device, (2) each mobile user device generates its own first public-private key pair (and a backup or second public-private key pair) and wirelessly distributes *a plurality of shares of* the second private key *to a plurality of different entities* once such that the second private key can be *re-created by the mobile user device to replace use of the first private key and deactivate the first private key when the second private* *key is re-created* and (3) wirelessly transmitting the second public key to a verifier device *concurrent with the first public key.* By transmitting the second public key concurrently with the first public key, the second public key is transmitted at about the same time as the public key and to the same receiver.

The Office Action relies on O'Shea to teach the limitation of "creating the keys at a mobile device, wirelessly transmitting the keys, and then authenticating at the mobile device". O'Shea is directed to methods and systems for unilateral authentication of messages based on a sender's address, public key and a digital signature. The sender provides information including content data, the public key, the address, and the digital signature generated using the private key corresponding to the public key. Upon reception, the recipient verifies the address by recreating it from the public key. The signature is verified using the network address and public key. The recipient accepts the content data when both the address and signature are verified. (See Abstract)

Nowhere does O'Shea teach *distributing a plurality of shares* of the second private key are wirelessly transmitted to *a plurality of different entities once,* such that the second private key can be *re-created by the mobile user device to replace use of the first private key* and *disable the first private key when the second private key is re-created* as in amended claims 1, 11, 14, 19, 22, 26, 50 and 51.

Hollis also fails to disclose distributing *a plurality of shares of* the second private key *to a plurality of different entities.* Hollis uses an "offline backup" system to store the backup key (Col. 24, line 41) which is intended to *restrict distribution* of such backup key. In other words, in Hollis, the key is sent to a backup system so that it doesn't have to be distributed to multiple users.

With regard to *concurrent transmission of the first and second public keys*, the Office Action relies on Hollis, col. 24, lines 5-7, as teaching concurrent transmission of the first and second public keys as claimed. However, Hollis fails to disclose concurrent transmission of the first and second public keys. In fact, Hollis discloses that the second public key is *backed up offline* (Col. 24, line 41), which indicates that it is not transmitted at all. In fact, the use of the words "offline back up" appears to indicate that the second public key in Hollis is not transmitted over the network at all but may be, perhaps, manually accessed or conveyed. Also, Hollis fails to explicitly recite whether the second public key is ever transmitted, since such _off line backup_ may simply store the keys. By contrast, the claims explicitly recite *concurrent transmission of the first and second public keys,* i.e. the first and second public keys are transmitted at about the same time and to the same receiver. As the *second public key is* _*not transmitted*_, the second public key _*cannot be transmitted concurrently*_ *with the first public key.*

Consequently, neither Hollis nor O'Shea, either alone or in combination, teach all the limitations of amended claims 1, 11, 14, 19, 22, 26, 50 and 51.

Scope and Content of Cited Prior Art References and Level of Skill in the Art Do Not Provide Motivation To Combine References

Assuming, arguendo, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Hollis and O'Shea as alleged in the Office Action.

The Office has the burden to show that one of ordinary skill in the art could have combined the elements claimed by known methods, and that in combination; each element would have merely performed the same function as it did separately. "In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." In re Linter, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972).

Even if the references were combined, albeit improperly in Applicant's opinion, as described above, Applicants submit that the combination of the references does not teach or suggest the mobile user device of independent claims 1, 11, 14, 19, 22, 26, 50 and 51.

The Office Action states that "it would have been obvious …to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been that the heavy cost may impede the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks."

A careful review of the section cited by the Office Action, (page 1, paragraph 6), as well as the entire reference, reveals that O'Shea is merely discussing that one perceived difficulty in *implementing the* *__authentication__* *functionality* is that IPsec and other authentication servers provide their security by means of quite complicated mechanisms that come as a heavy price or cost and not that the growth of mobile networks would be impeded as suggested by the Office Action.

Furthermore, as discussed above, Hollis makes it clear that the second key pair is an *offline back up* (Col. 24, line 41) and fails to disclose how or if this second key pair is ever transmitted by a mobile user device. In fact, the use of the words "offline back up" appears to indicate that the second key pair in Hollis is not transmitted over the network at all but may be, perhaps, manually accessed or conveyed. Also, Hollis fails to explicitly recite whether the second key pair is ever transmitted, since such *off line backup* may simply store the keys. As the second key pair is backed up by keeping them *"offline"*, Hollis teaches away from wireless transmission of the second key pair. Consequently, there is not motivation to combine Hollis which backs up the second key pair offline with O'Shea which transmits keys wirelessly.

Based on these references, there is no clear guidance of whether an online (i.e. connected to or served by the system) or offline system (i.e. __not__ connected to or served by the system) should be utilized and how the opposite teachings can even be combined without a wholesale redesign or restructuring of the offline key security system taught by Hollis.

Furthermore, Hollis is aimed at securing data communications as it travels across rendezvous points (RVP) (nodes, servers) of a public data network by using a public-private key pair between each node to *encrypt communications*. Applicant submits that "authentication" in O'Shea is distinct from the encryption system described by Hollis. With authentication the recipient is able to determine whether the sender is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, the motivation supplied by the Office Action of combining Hollis and O'Shea is improper as the motivation is directed to reducing administrative and communicative overhead *in implementing authentication functionality* while Hollis is *directed to encryption algorithms to minimize the threat of eavesdropping* (See column 2, lines 30-37). Additionally, there is no reasonable expectation of success in combining these two references.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to the limitation of a wireless apparatus as recited in claims 1, 11, 14, 19, 22, 26, 50 and 51.

Claims 29, 33, 40, 43 and 47

As to independent claims 29, 33, 40, 43 and 47, Office Action cites Schwenk as teaching the claimed invention except for "creating the keys at a mobile device, wirelessly transmitting the keys, and then authenticating at the mobile device."

Differences Between Prior Art and Claims: Claimed Elements are Not Taught by the Prior Art

Applicant submits that neither Schwenk nor O'Shea teach the claimed limitations where a mobile user device is authenticated by a network verifier device where each mobile user device generates its own private key, public key corresponding to the private key, and *an associated system parameter* and *wirelessly outputting the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device.*

Schwenk is directed to a method for generating and regenerating an encryption key. In particular, Schwenk discloses an algorithm for allowing a user to reconstruct an encryption key by storing regeneration information at a trusted center. Although Schenk discloses a public parameter "g", this parameter is stored at both the user and trust center and is used by the trust center to generate the public key. The parameter is used to generate the public key at the trust center, the user already has a copy of the public parameter "g" (see column 4, lines 42-45), and the trust center transmits the public key to the user (see Figure 1 and column 4, lines 42-45). Thus, Schwenk fails to teach, disclose or suggest a mobile user device generating its own private key, a public key corresponding to the private key, and *an associated system parameter* and *wirelessly outputting the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device* as claimed. In Schwenk, no system parameter is sent to the verifier device *concurrent* with the transmission of the public key. O'Shea fails to make up for this deficiency.

Scope and Content of Cited Prior Art References and Level of Skill in the Art Do Not Provide Motivation To Combine References

Assuming, arguendo, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Schwenk and O'Shea as alleged in the Office Action.

Even if the references were combined, albeit improperly in Applicant's opinion, as described above, Applicants submit that the combination of the references does not teach or suggest the mobile user device of independent claims 29, 33, 40, 43 and 47.

The Office Action states that "it would have been obvious ...to modify the key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been to be able to reconstruct the key in the event it is lost (Schwenk, column 5, line 55)." As there is no column 5, line 55 in Schwenk, Applicant believes that the Office Action may have meant to refer to Column 2, lines 65-67 of Schwenk which states "to render possible the reconstruction of this key pair U and C, regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss".

As discussed above, Schwenk is directed to a method for generating and regenerating an encryption key. Consequently, Schwenk is focused on *"encryption" keys*. (See Col. 2, lines 28-67). On the other hand, O'Shea, as discussed above, is directed to methods and systems for *unilateral authentication of messages* based on a sender's address, public key and a digital signature. Applicant submits that "authentication" in O'Shea is distinct from the encryption system described by Schwenk. With authentication the recipient is able to determine whether the sender is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, there is no motivation to combine a system for authentication with a system for encryption.

As these cited prior art references operate on different communication architectures which combination is structurally and/or operationally incompatible with each other, Applicants submit that one of ordinary skill would not be motivated by the teachings of O'Shea to modify Schwenk to develop a mobile user device which is authenticated by a network verifier device where each mobile user device generates its own private key, public key corresponding to the private key, and *an associated system parameter* and *wirelessly outputting the system parameter to a verifier device* *concurrent* *with wirelessly outputting the public key to the verifier device* as in independent claims 29, 33, 40, 43 and 47.

Should the Office Action maintain the position that it would have been obvious to one of ordinary skill in the art to modify and combine these references, Applicants respectfully request that a detailed explanation of how these structurally and operationally different communication architectures can be modified in view of their incompatible operation.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to the limitation of a wireless apparatus as recited in claims 29, 33, 40, 43 and 47.

Claims 3, 16 and 24

As to dependent claims, 16 and 24, Office Action cites Hollis and O'Shea as teaching the claimed invention except for the "recreation of the second private key."

Differences Between Prior Art and Claims: Claimed Elements are Not Taught by the Prior Art

Applicant submits that Hollis, O'Shea or Schneier fail to teach the claimed limitations occurring in a system where mobiles user devices are authenticated by a network verifier device.

The Office Action cites Hollis and O'Shea as teaching using the second private key for authentication (Hollis, column 10, line 23). (See page 9 of Office Action) As discussed above, Hollis is directed to securing message oriented network communications using *standard encryption algorithms and not by authentication* as in the present claimed invention. Therefore, Hollis fails to teach using a second private key for authentication.

The Office Action cites Schneier as teaches reconstructing keys as in the claimed present invention. Applicants respectfully disagree. In the claimed invention, the key is re-created at the mobile user device (See independent claim 1 from which claim 3 depends). In other words, the user can re-create the key with the cooperation of the parties that receive a share of the key, *while* *none of the parties that receive a share of the keys can recreate the key alone.* (See paragraph [0037] of the published application)

. Schneier, on the other hand, is directed to a method of dividing up a key into some number of pieces and then sending each piece encrypted to a different company office. This protects the user (Alice in the case of the Schneier reference) against any one malicious person and the employer is protected against losing all of Alice's data. This is because someone can gather all the pieces and reconstruct the key. In other words, *anyone can reconstruct the key in Schneier* whereas in the present claimed invention, only the user can re-create the key. The present invention, on the other hand, is directed at preventing any *of the parties that receive a share of the keys from recreate the key alone.* (See paragraph [0037] of the published application). Consequently, Schneier fails to teach "recreation of the second private key" as in the claimed present invention.

Scope and Content of Cited Prior Art References and Level of Skill in the Art Do Not Provide Motivation To Combine References

As described above, there is no motivation to combine Hollis and O'Shea. With regard to combining Hollis and Schneier, the Office Action states that it would be "obvious to combine Hollis with Schneier because it is a more secure way to protect a backup key (page 182, 2nd paragraph". (See page 2 of Office Action)

While it may be a more secure way to back up a key, it does not provide the motivation to combine Hollis and Schneier as alleged in the Office Action. The systems in Hollis and Schneier are different. Hollis uses an "offline backup" system (i.e. not connected to or served by the system) to store the backup key (Col. 24, line 41) which is intended to restrict distribution of such backup key. In other words, the key is sent to a backup system so that it doesn't have to be distributed to multiple users as is the case in Schneier. Consequently, Hollis teaches away from the distribution of keys in Schneier.

Hollis secures the backup keys by keeping them *"offline"* (i.e. not connected to or served by the system) and transmitting to *a single location* while Schneier secures its backup key by transmitting it *online (i.e. connected to or served by the system) in pieces to different entities.* While both of these approaches protect the backup key, there is no explicit motivation to modify the teachings of Hollis to go from *offline* storage of the backup keys to the *online* distribution of the backup keys to different entities as in Schneier.

Based on these references, there is no clear guidance of whether an online or offline system should be utilized and how the opposite teachings of each reference can even be combined without a wholesale redesign or restructuring of the offline key security system taught by Hollis with the opposing online key security system taught by Schneier.

Consequently, there is no reasonable expectation of success in combining these two references.

Claims 4 and 2

Dependent claims 4 and 25 are directed to disabling the first private key by using the second private key for authentication.

Differences Between Prior Art and Claims: Claimed Elements are Not Taught by the Prior Art

Applicant submits that Hollis, O'Shea or Schneier fail to teach the claimed limitation of *disabling* the first private key by using the second private key for authentication.

The Office Action cites Hollis as teaching "disabling the first private key when the second is used for authentication (Hollis, column 14, lines 46-48)." Applicants respectfully disagree. In the claimed invention, the first private key is *disabled*, i.e. the first private key is made incapable of being used or ineffective. Hollis, on the other hand, teaches *removing* the public key. Specifically, Hollis states, "[a]lso, if the key was present but incorrect, the offending key *is removed* from the Keys Database 124". As removing the public key is different than disabling the public key, Hollis fails to teach this limitation.

O'Shea and Schneir fail to make up for the deficiencies of Hollis. Consequently, prima facie obviousness has not been established as to these claims.

Claims 2, 5-10, 12-13, 15, 17-18, 20-21, 23, 27-28, 30-32, 34-35, 37-39, 41-42, 44-46 and 48-49

The remaining claims 2, 5-10, 12-13, 15, 17-18, 20-21, 23, 27-28, 30-32, 34-35, 37-39, 41-42, 44-46 and 48-49 were rejected based on a combination of references, some of which are discussed above. Applicant submits that none of the cited prior art references teach the wireless distribution of a (backup) second public key from a mobile device concurrent with the wireless distribution of a first public key as claimed. The arguments and differences disclosed above apply equally to these claims and make the patentable over the cited prior art. In particular, none of the references disclose a system and method for *authentication* of subscriber user devices (e.g., mobile phones) with a network verifier where each mobile user device generates its own first public-private key pair (and a backup or second public-private key pair) and wirelessly distributes the public key to the verifier for future *authentication* of the mobile user device. A *plurality of shares* of the second private key are wirelessly transmitted to *a plurality of different entities once* such that the second private key can be *re-created by the mobile user device to replace use of the first private key* and *disable the first private key when the second private key is re-created*. Additionally, none of the cited prior art references teach a mobile user device is authenticated by a network verifier device where each mobile user device generates its own private key, public key corresponding to the private key, and *an associated system parameter* and *wirelessly outputting the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device* as claimed.

Based on at least the foregoing reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of, and/or objection and allowance of claims 1-51.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests **a one month** extension of time in which to respond to the Office Action dated July 3, 2008. Please charge extension any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: November 3, 2008

By: Won Tae C.

Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502